Digital Security
Progress. Protected.

מאגר שאלות לדוגמא למבדק אבטחה פנימי

התייחסו לשאלות לדוגמא הבאות, ככלי שיעזור לכם לבנות את מבדק האבטחה הפנימי של החברה שלכם. באמצעות תוספות ושינויים בהתאמה למאפיינים הספציפיים של החברה שלכם, הן יוכלו לעזור לכם לזהות את הפערים והאתגרים שמולם צריך להשקיע מאמצים נוספים.

1. מה עליך לעשות במקרה של חשיפת סיסמא הקשורה לחברה? (בחרו בכל האפשרויות הנכונות)
א. שום דבר.
ב. לשנות את הסיסמא באופן מיידי.
ג. לדווח על דליפת הסיסמא כתקרית אבטחה.
ד. לראות אם קורה משהו.

התשובות הנכונות: ב׳, ג׳
מידע נוסף: כפי שכתוב במסמך מדיניות האבטחה לעובדים (הכנס קישור למדיניות האבטחה של החברה), בכל מקרה של חשיפת סיסמא, על העובד לשנות את הסיסמא באופן מיידי ולדווח על תקרית האבטחה.

2. מהו ההליך הנכון מבחינת אבטחה במקרה של אובדן מפתח, כרטיס חכם או תג עובד?
א. להיכנס למשרדי החברה ללא אימות יחד עם החברים לעבודה או לשאול תג עובד/כרטיס חכם מחבר לעבודה.
ב. לחכות זמן מה (שבוע, למשל), ואם תג העובד/הכרטיס החכם לא נמצא עד אז, לדווח על אובדן.
ג. לדווח על אובדן המפתח/הכרטיס החכם באופן מיידי.
ד. לבקש תג עובד/כרטיס חכם שמיועד למבקרים ולהשתמש בו.

התשובה הנכונה: ג׳
מידע נוסף: חשוב לדווח באופן מיידי על אובדן תג עובד/כרטיס חכם כך שיהיה אפשר לחסום אותו וכתוצאה מכך למנוע שימוש לרעה וכניסה לא מאושרת למשרדי החברה.

3. כיצד אוכל לשמור על סודיות של מידע רגיש שנשלח בדוא״ל?
א. אפשר להוסיף הצהרת ויתור סודיות בתחתית ההודעה.
ב. בשום אופן, ולכן – אין לשלוח מידע רגיש בדוא״ל בשום מקרה.
ג. אפשר להצפין את ההודעה.
ד. אפשר לחתום על ההודעה.

התשובה הנכונה: ג׳
מידע נוסף: תוקף יכול ליירט את הודעות הדוא״ל שלכם – או מתוך שרת הדוא״ל או במהלך העברת ההודעה. החותמת הדיגיטלית מעידה שהתוכן של ההודעה לא שונה במהלך ההעברה, אך היא לא הופכת את ההודעה ללא-קריאה. הצפנה הופכת את ההודעה ללא-קריאה מרגע שנשלחה ועד לרגע שהנמען המיועד פותח אותה. ניתן להשתמש באפשרויות הצפנה המבוססות על אישורים דיגיטליים ומותקנות בשירות הדוא״ל שלכם, או בתוכנות הצפנה חיצוניות.

4. כיצד המחשב יכול להידבק בנוזקה? (בחרו בכל האפשרויות הנכונות)
א. באמצעות הפעלת נוזקה שנראית כמו תוכנה לגיטימית.
ב. באמצעות ביקור באתר אינטרנט שהודבק בנוזקה.
ג. באמצעות דוא״ל – הודעת דוא״ל בפורמט HTML או באמצעות קבצים מצורפים (קבצי אופיס, PDF).
ד. באמצעות התחברות לרשת שהודבקה בנוזקה – במלון, רכבת, אוטובוס או ברשת אלחוטית חינמית.

התשובות הנכונות: א׳, ב׳, ג׳, ד׳

מידע נוסף: הרצת נוזקה שנראית כמו תוכנה או אפליקציה לגיטימית, ביקור באתר אינטרנט שהודבק בנוזקה, פתיחת הודעת דוא״ל והתחברות לרשת שהודבקה בנוזקה הן דרכים פופולריות להדבקה של מחשב בנוזקה.

5. כיצד אפשר לצמצם את כמות דואר הזבל (ספאם) בתיבת הדוא״ל הארגונית? (בחרו בכל האפשרויות הנכונות)
א. יש להימנע משימוש בכתובת הדוא״ל הארגונית בזמן הרשמה לשירותים שאינם קשורים לעבודה.
ב. פרסום כתובת הדוא"ל הארגונית בפורומים ציבוריים.
ג. הרשמה לניוזלטרים אמינים בלבד.
ד. שימוש בכתובת הדוא״ל הארגונית לפעילויות הקשורות לעבודה בלבד.

התשובות הנכונות: א׳, ג׳, ד׳
מידע נוסף: אם אתם רוצים לצמצם את כמות דואר הזבל (ספאם) שמגיעה לתיבת הדוא״ל הארגונית, עליכם להיזהר מפני הפצת כתובת הדוא״ל באתרים ציבוריים, בחדרי צ׳אט, בפורומים ציבוריים, ברשתות חברתיות וכן הלאה. עליכם להשתמש בכתובת דוא״ל אחרת בכל מקרה בו אתם צריכים להשתמש בדוא״ל לפעילויות האישיות שלכם. השיבו להודעות דוא״ל רק אם הן נראות לכם לגיטימיות. אם תוכן ההודעה או השולח עצמו נראים לכם חשודים, וודאו שההודעה אמינה לפני שתשיבו לה. אותו הכלל חל גם על ביטול הרשמה לרשימות תפוצה. תגובה לדואר זבל מוכיחה לשולח שכתובת המייל שלכם פעילה ולגיטימית.

6. מה מהבאים כדאי לעשות כדי להימנע מהידבקות בווירוסים ונוזקות ?
א. להוריד תוכנות ממקורות אמינים בלבד.
ב. להתקין תוכנת אנטי-וירוס.
ג. עדכנו את המחשב בכל מקרה בו מופיעה הודעת עדכון מהמערכת.
ד. כל התשובות נכונות.

התשובה הנכונה: ד׳
מידע נוסף: כל האפשרויות רלוונטיות כדי למנוע הדבקה של המחשב בווירוסים ונוזקות.

7. היכן יש לשים את מכשירי החברה (מסכים, מחשבים ניידים) אם הם משמשים לעיבוד מידע שמוגדר כ״סודי״ או ״סודי ביותר״?
א. זה לא משנה.
ב. בקרבת חלון.
ג. בקרבת דלתות.
ד. במקום בו אנשים לא מורשים, לא יוכלו לראות את המידע הרגיש

התשובה הנכונה: ד׳
מידע נוסף: יש למקם מכשירים שבהם מתבצע עיבוד מידע ״סודי״ או ״סודי ביותר״ במקום בו הסיכון לצפייה במידע המסווג דרך מסכים יצטמצם ככל האפשר.

8. אחרי אילו חוקים/כללים יש לעקוב בזמן שימוש במכשירי טלפון של הארגון? (בחרו בכל האפשרויות הנכונות)
א. מדיניות נעילה ומדיניות סיסמאות לטלפונים ניידים.
ב. הצפנת טלפונים ניידים וכרטיסים.
ג. התקנת כל האפליקציות האפשריות.
ד. כל התשובות נכונות.

התשובות הנכונות: א׳, ב׳
מידע נוסף: הרגלים בריאים יחד עם מדיניות ניהול מכשירים ניידים (MDM) תורמים להגנה על הנתונים המאוחסנים בטלפונים ניידים מפני גישה לא מורשית, באמצעות שימוש בכלי הבקרה הבאים:
1. מדיניות נעילה ומדיניות סיסמאות לטלפונים ניידים
2. הצפנה של הטלפונים הניידים (ושל הכרטיסים, אם הטלפון הנייד משתמש בכרטיס) וחסימת השימוש בתוכנות ממקורות לא-בטוחים (iTunes, Google Play וה-MDM Market).
בזמן התקנת אפליקציה, בחרו באפליקציות הוותיקות יותר – ברוב המקרים הורידו אותן יותר והן מקבלות דירוגי אמינות גבוהים יותר.

9. אתם גולשים באתר אינטרנט דרך רשת אלחוטית ציבורית (Wi-Fi), אך תוכנת האנטי-וירוס שלכם לא מעודכנת. אילו מההיגדים הבאים נכון?
א. המכשיר שמחובר לרשת אלחוטית ציבורית עדיין מאובטח, מכיוון שאתם יכולים לגשת רק לדפי אינטרנט שכוללים חדשות מהמדינה שלכם.
ב. לא ניתן לצותת לתקשורת בפרוטוקול HTTP.
ג. התקשרות למערכות ארגוניות דרך VPN היא בטוחה.
ד. אף אחת מהתשובות אינה נכונה.

התשובה הנכונה: ד׳
מידע נוסף: HTTP הוא פרוטוקול המשמש לתקשורת בין שרת אינטרנט ובין דפדפן. הפרוטוקול לא מגן על הסודיות של המידע המועבר בו וניתן לצותת לו. ניתן להדביק את המחשב בנוזקות גם בגלישה רגילה באתרי אינטרנט לגיטימיים, והסיכוי להדבקה גדל אם האנטי-וירוס, הדפדפן או מערכת ההפעלה אינם מעודכנים. זה נכון גם בנוגע לתקשורת דרך VPN.

10. אילו מהאפשרויות הבאות עוזרות לקבוע אם אתר לרכישות מקוונות הוא אמין?
א. כתובת האתר מתחילה ב-"https://".
ב. יש חותמת על האתר שעליה כתוב "בטוח ב-100%".
ג. מחקר קצר על האתר לבדיקה האם המוניטין שלו טוב
ד. קריאה באתר וחיפוש ביקורות חיוביות מלקוחות.

התשובה הנכונה: ג׳
מידע נוסף: אתרים זדוניים יכולים לפעול גם בפרוטוקול HTTPS, וניתן לזייף חותמות אבטחה בקלות. בעלי האתר יכולים לשים ביקורות מזויפות של לקוחות באתר שלהם. האפשרות הטובה ביותר היא לבצע מחקר קצר כדי לראות אם לאתר יש מוניטין טוב. מוניטין הוא חשוב מאוד בזמן קניות באינטרנט. אמינות האתר היא שיקול חשוב מאוד ויש לתת לו עדיפות בתוך כלל השיקולים שלפיהם אתם בוחרים אתר לרכישות מקוונות.

11. במה מהבאים משתמשים במתקפת הומוגליפים או הומוגרפים?
א. התוקף מנצל דמיון באופן הכתיבה של אותיות שונות.
ב. התוקף שולח קובץ מצורף שמודבק בנוזקה.
ג. התוקף שולח את אותה הודעת פישינג לכל האנשים בחברה.
ד. אף אחת מהתשובות אינה נכונה.

התשובה הנכונה: א׳
מידע נוסף: תוקפים החלו להשתמש בטקטיקות חדשות כדי לבלבל משתמשים. הטקטיקה הזאת נקראת ״הומוגליפים״. מתקפת הומוגליפים מתבססת על החלפת אות אחת בכתובת האינטרנט באות דומה, או אף באות זהה שהיא חלק משפה אחרת. העין האנושית לא מצליחה להבחין בהבדל, אך מחשב שמתייחס לכל אות שכתובה עם קוד שונה יודע להבדיל ביניהן.

12. אילו מפעולות השימוש בסיסמאות הבאות הן בטוחות?
א. מסירת הסיסמא למנהל שלכם לפי דרישה.
ב. שמירת הסיסמא באמצעות כלי של ניהול סיסמאות שרק לך יש את הגישה אליו.
ג. מסירת הסיסמא לצוות האבטחה הפנימי לפי דרישה.
ד. כתיבת הסיסמא על פיסת נייר והדבקה שלה לחלק האחורי של המקלדת.

התשובה הנכונה: ב׳
מידע נוסף: סיסמא שמשותפת עם אנשים לא-מורשים אינה בטוחה, לא משנה מה האורך שלה, המורכבות שלה, או כל מאפיין אחר שתורם לחוזק שלה.

13. באילו דרכים משתמשים רשאים להשתמש בסיסמאות שלהם *בחברת (שם החברה)*?
א. אין מגבלות.
ב. הסיסמאות חייבות להיות מורכבות. משתמשים רשאים להשתמש בסיסמאות שלהם ב***(שם החברה)*** גם מחוץ ל***(שם החברה)***.
ג. הסיסמאות חייבות להיות מורכבות. משתמשים אינם רשאים להשתמש בסיסמאות שלהם ב***(שם החברה)*** גם מחוץ ל***(שם החברה)***.
ד. הסיסמאות חייבות להיות מורכבות. משתמשים רשאים לחלוק את הסיסמאות שלהם עם חברים לעבודה.

התשובה הנכונה: ג׳
מידע נוסף: עובדים מוכרחים ליצור סיסמאות מורכבות שיהיו ארוכות מספיק כך שתוקף לא יוכל לנחש אותן. ישנן גישות רבות ליצירת סיסמא חזקה. אחת מהן היא לזכור משפט, למשל –
״I need five coffees to deliver the code today״, ולאחר מכן לשנות את האותיות למספרים ו/או לבחור את האות הראשונה/השנייה/האחרונה בכל מילה. כך, המשפט -
״I need five coffees to deliver the code today״
הופך ל-״I need 5 coffees 2 deliver the c0d3 today״
שהופך ל-״In5c2dtc2day״.
השיטה ליצירת הסיסמא והמשפט המקורי ממנו נוצרה הסיסמא צריכים להיות ידועים אך ורק למשתמש בסיסמא. אין להשתמש מחוץ ל(שם החברה) בסיסמא שמשמשת לגישה למערכות מידע בתוך (שם החברה). אל תשתפו את הסיסמא שלכם עם אף אחד: לא עם החברים לעבודה, לא עם בני המשפחה, לא עם המנהל ולא עם צוות ה-IT. אל תגלו את הסיסמא שלכם לאנשים גם אם אתם בחופשה ומישהו אומר לכם שהם חייבים לגשת בדחיפות למערכת. צוות ה-IT נמצא כאן כדי לטפל במצבים כאלה.

14. אתם מקבלים שיחה, והמתקשר מבקש מידע רגיש. כיצד יש להגיב?
א. לבקש מהמתקשר לשלוח את הבקשה באמצעות הודעת דוא"ל חתומה מכתובת ארגונית ולוודא את זהות המתקשר.
ב. להתעקש שתתקשר אליהם בחזרה.
ג. לבקש את שמו של המנהל שלהם לפני היענות לבקשה.
ד. להיענות לבקשה מכיוון שהם עובדים מהבית ואין להם גישה לטלפון עסקי.

התשובה הנכונה: א׳
מידע נוסף: דיוג קולי (Vishing) הוא ניסיון להשתמש בהנדסה חברתית דרך טלפון כדי להוציא מידע אישי או רגיש ממשתמש או לגרום לו לבצע פעולות מסוימות – למשל, התקנת תוכנת להשתלטות מרחוק ומתן הרשאה ל"טכנאי" לתקן את המחשב. עליכם לבקש מהמתקשר לשלוח כל בקשה לקבלת מידע רגיש באמצעות הודעת דוא"ל חתומה מכתובת ארגונית ולוודא את זהותו של המתקשר לפני מתן תשובה להודעה. אם האדם מספק מספר טלפון לחזרה או את המספר של המנהל שלו, זה עשוי להיות חלק מהתרמית, ולכן אל תשתמשו בו. במקום זאת, חפשו את מספר הטלפון של החברה והתקשרו לארגון הרלוונטי.

15. מהי הדרך הטובה ביותר להגנה על פרטיותם של נתונים שמאוחסנים במחשב נייד גם במקרה שהוא נגנב?
א. הצפנה מלאה של הכונן הקשיח.
ב. כלי נגד גניבה.
ג. אנטי-וירוס.
ד. גיבוי.

התשובה הנכונה: א׳
מידע נוסף: הדרך הטובה ביותר להגנה על נתונים היא הצפנה מלאה של הכונן הקשיח. כלי נגד גניבה עשוי לעזור באיתור המחשב והחזרתו, אך הגנב יכול לגשת למידע בכונן הקשיח אם הוא אינו מוצפן. פתרון להגנה מפני נוזקות לא עוזר במקרה של גניבה פיזית. גיבוי הוא אמצעי ששומר על זמינות של מידע, אך לא על הסודיות שלו.

16. האם מותר להעלות, לאחסן ולעבד מידע מסווג של החברה בשירותי ענן לא מאושרים (Google Docs, Google Translate, Google Drive, Dropbox וכו׳)?
א. כן.
ב. לא.

התשובה הנכונה: ב׳
מידע נוסף: ניתן לאחסן ולעבד מידע מסווג רק בשירותי ענן של ספקים שאושרו ע"י (שם החברה). ישנן קטגוריות ספציפיות של נתונים מסווגים אותן אסור לעבד גם בשירותי ענן מאושרים.

17. איזה מידע אסור לשתף בפרופיל אישי ברשת חברתית? (בחרו את כל התשובות הנכונות)
א. מידע על הפעילות הפנימית של החברה.
ב. כתובות דוא"ל ארגוניות ופרטי קשר אחרים.
ג. סיפורים מצחיקים על דברים שקרו לכם במהלך חופשות.
ד. המידע האישי שלכם – כתובת, מס. זהות וכו'.

התשובות הנכונות: א׳, ב׳, ד׳
מידע נוסף: מידע על הפעילות הפנימית של החברה, כתובות דוא"ל ארגוניות ופרטי קשר אחרים, ומידע אישי כמו כתובת, מס. זהות וכו׳ הם מידע רגיש ואסור לחשוף אותם.

18. מדוע עליכם לנעול את מסך המכשיר כשאינו בשימוש?
א. כדי למנוע התקנה אוטומטית של קוד זדוני.
ב. כדי למנוע שימוש לרעה בהרשאות הגישה שלכם ע"י אנשים לא-מורשים במטרה לגשת למידע שעל המכשיר.
ג. כדי לגבות נתונים מהמכשיר באופן תקין.
ד. כדי לעמוד בחוקי ההגנה על זכויות יוצרים.

התשובה הנכונה: ב׳
מידע נוסף: אם המכשיר אינו נעול (כלומר אינו דורש קוד אישי או סיסמא כדי להמשיך לפעול), כל אדם שיכול לשלוט בו מקבל הרשאות דומות לאלו של המשתמש המקורי במכשיר. המשמעות של זה היא שמתחזה יוכל לקבל גישה לכל הנתונים המאוחסנים במכשיר.

19. אילו מהאפשרויות הבאות *אינן* פרקטיקות טובות להגנה פיזית?
א. העובדים מוכרחים לבצע נעילה למחשב כשהן לא מול המחשב.
ב. העובדים מוכרחים להיצמד לעקרונות מסך נקי ושולחן נקי.
ג. העובדים מוכרחים לבצע תחזוקה מונעת ותיקונים במכשירי החברה.
ד. לעובדים אסור לעבוד עם מידע רגיש באזורים בהם אנשים לא-מורשים עשויים להיחשף אליו

התשובה הנכונה: ג׳
מידע נוסף: פרקטיקות האבטחה המומלצות אומרות שבכל מקרה של הפסקת עבודה עם המחשב / המכשיר הנייד, על העובד לנעול אותו כך שתידרש התחברות מחדש כדי לחזור לעבודה; על העובד להיצמד לעקרונות מסך נקי ושולחן נקי; וכן אסור לעובד לעבוד עם מידע רגיש באזורים בהם אנשים לא-מורשים עשויים להיחשף אליו. בניגוד לכך, תחזוקה מונעת ותיקונים במכשירי החברה צריכים להתבצע אך ורק על ידי אנשי שירות מורשים ולא על ידי העובדים.

20. כיצד אתם מעריכים את רמת המודעות שלכם לנושאי אבטחה?
א. מצוינת.
ב. טובה.
ג. חלשה.
ד. חסרה.